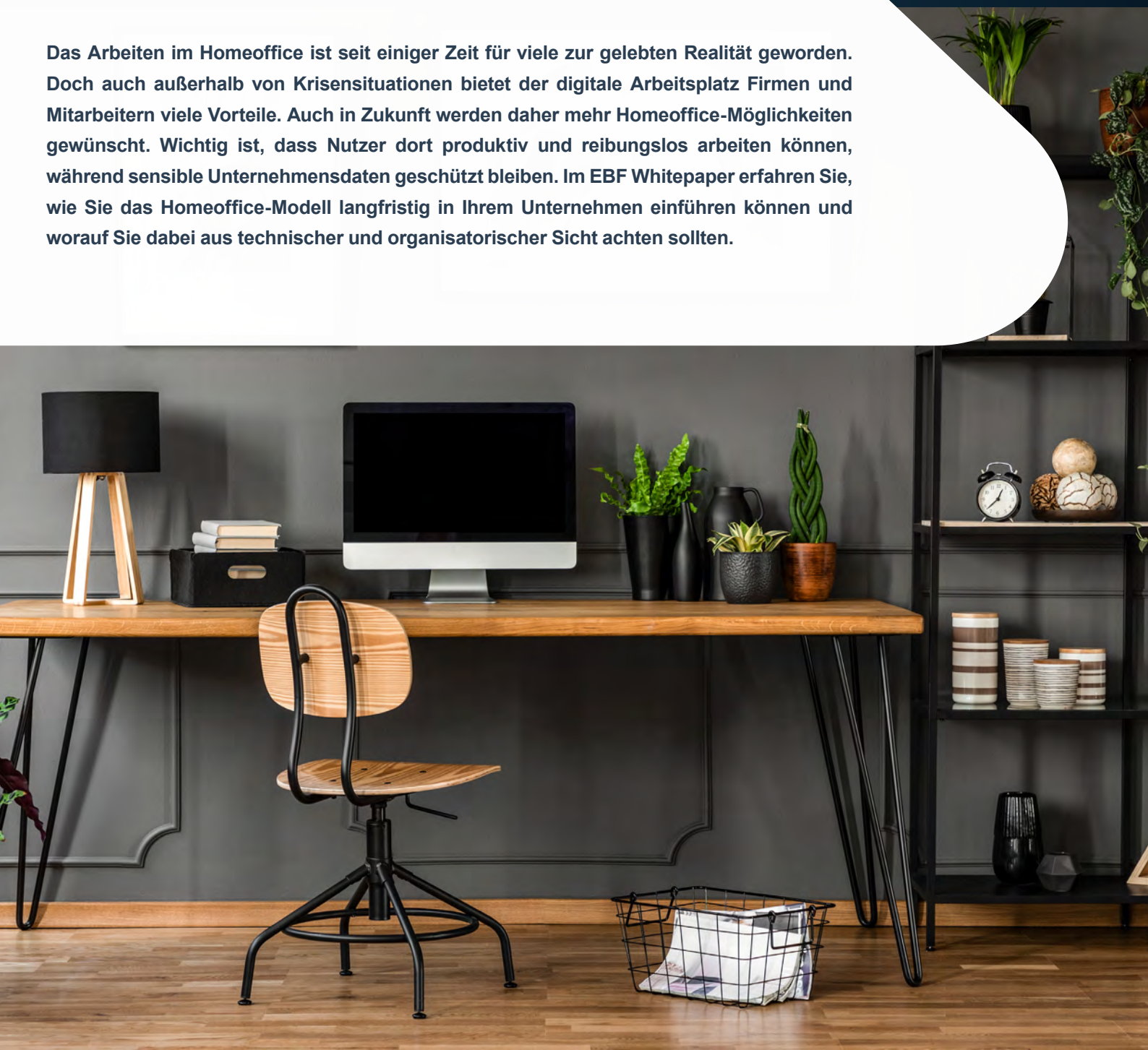
Whitepaper

# HOMEOFFICE UND REMOTE WORK EINFÜHREN — SO GEHT'S

**Das Arbeiten im Homeoffice ist seit einiger Zeit für viele zur gelebten Realität geworden. Doch auch außerhalb von Krisensituationen bietet der digitale Arbeitsplatz Firmen und Mitarbeitern viele Vorteile. Auch in Zukunft werden daher mehr Homeoffice-Möglichkeiten gewünscht. Wichtig ist, dass Nutzer dort produktiv und reibungslos arbeiten können, während sensible Unternehmensdaten geschützt bleiben. Im EBF Whitepaper erfahren Sie, wie Sie das Homeoffice-Modell langfristig in Ihrem Unternehmen einführen können und worauf Sie dabei aus technischer und organisatorischer Sicht achten sollten.**



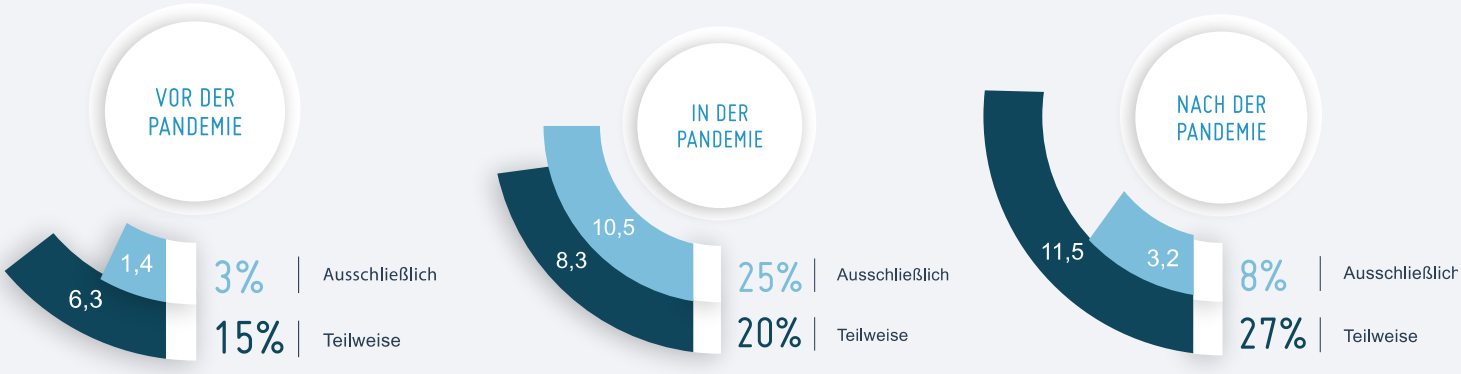
# 1 Corona macht Homeoffice massentauglich

Vor der Coronapandemie war Homeoffice in vielen Unternehmen noch die Ausnahme.
Durch die positiven Erfahrungen im Lockdown möchten viele Mitarbeiter auch nach der Corona-Pandemie gelegentlich aus dem Homeoffice arbeiten.

Denn die flexible Wahl des Arbeitsplatzes hat viele Vorteile. Und zwar nicht nur für Arbeitnehmer, sondern auch für Arbeitgeber. Mitarbeiter können ihre tägliche Arbeit zu Hause flexibel und entlang ihrer individuellen Bedürfnisse gestalten. Das schafft ein effizientes und produktives Arbeitsklima und sorgt für eine erhöhte Mitarbeiterzufriedenheit sowie eine stärkere Bindung an den Arbeitgeber.

Unternehmen auf der anderen Seite profitieren von der erhöhten Produktivität und Motivation ihrer Mitarbeiter und können durch agile Arbeitsmöglichkeiten besser auf Veränderungen reagieren. Das Homeoffice-Angebot sorgt zudem für einen Anstieg der Arbeitgeberattraktivität: So ziehen insbesondere Berufsanfänger und Young Professionals mobile Arbeitsmöglichkeiten als Kriterium bei ihrer Arbeitgeberwahl heran. Ein weiterer Vorteil besteht darin, dass Unternehmen deutlich mehr potentielle Mitarbeiter erreichen können, wenn der Wohnort kein relevantes Kriterium beim Recruiting darstellt.

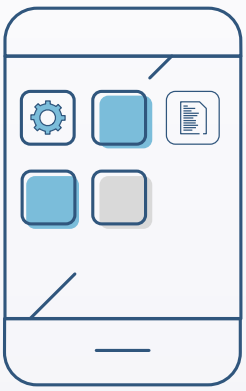
## Anteil der Berufstätigen im Homeoffice (in Mio)




*Quelle: Bitkom Research 2020, https://www.bitkom.org/Presse/Presseinformation/Mehr-als-10-Millionen-arbeiten-ausschliesslich-im-Homeoffice*

# 2 Homeoffice muss sicher und nutzerfreundlich sein

Mitarbeiter und Arbeitgeber können also von vielen Vorteilen profitieren. Voraussetzung dafür ist allerdings die richtige Umsetzung des Homeoffice-Modells. Hierfür müssen vor allem zwei wichtige Bedingungen erfüllt werden: Die Arbeit von zu Hause muss zum einen genauso sicher sein wie im Büro und sie muss zum anderen genauso komfortabel sein. Denn nur wenn Prozesse nutzerfreundlich gestaltet sind, führt dies auch zu einer erhöhten Produktivität und Zufriedenheit der Mitarbeiter. Dank moderner Technologien lässt sich beides gut vereinbaren.



3

## Grundlagen zur Realisierung des Homeoffice

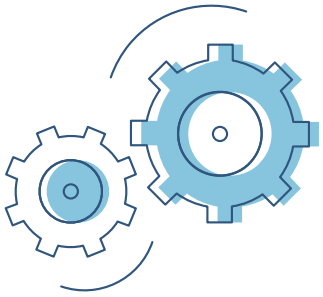
Im ersten Schritt müssen die individuellen Anforderungen des Unternehmens erfasst werden, um darauf aufbauend eine passende Strategie erarbeiten zu können. Dabei sollten sich Unternehmen beispielsweise über folgende Fragen Gedanken machen:

- **Welche Mitarbeitergruppen sollen wann und zu welchem Zweck aus dem Homeoffice arbeiten?**
- **Welche Tätigkeiten sollen zu Hause – neben dem Empfangen und Schreiben von Mails und Telefonaten – durchgeführt werden?**
- **Welche Prozesse lassen sich 1:1 im Homeoffice abbilden, bei welchen ist das nicht der Fall?**
- **Zu welchen Diensten und Systemen benötigen welche Mitarbeiter Zugriff?**
- **Welche Serverkapazitäten sind erforderlich?**
- **Welche Anforderungen stellen die Nutzer an Geräte, Anwendungen und deren Nutzerfreundlichkeit?**

4

## Richtige Gerätelandschaft

Als nächstes sollte die Frage geklärt werden, welche Geräte im Homeoffice zum Einsatz kommen sollen. Grundsätzlich ist dabei zu entscheiden, ob Mitarbeiter ausschließlich mit ausgegebenen Firmengeräten arbeiten sollen oder auch über private Geräte (Bring Your Own Device) auf Unternehmensanwendungen zugreifen dürfen.
Die Nutzung von Firmengeräten bietet den Vorteil, dass sowohl die Verwaltung als auch die Trennung von beruflichen und privaten Daten einfacher gelingt und die Komplexität der Gerätelandschaft gesteuert werden kann. Letzteres ist nicht der Fall, wenn auch BYOD-Geräte genutzt werden dürfen, da die Anzahl der unterschiedlichen Modelle und Betriebssysteme dann schwierig zu kontrollieren ist. Somit ist auch die Verwaltung der Geräte durch die Unternehmens-IT deutlich aufwändiger.
Sind in einem Unternehmen bisher aber beispielsweise keine Laptops oder Firmenhandys im Einsatz, so müssten hohe Investitionen für die Bereitstellung solcher Geräte getätigt werden. Unter anderem in einem solchen Fall kann die Einbindung privater Geräte eine Option sein. Denn auch sie lassen sich verwalten und berufliche und private Daten beispielsweise mittels Container-Lösung trennen.



## 5 Die passenden Betriebssysteme

Bei der Geräte-Strategie und notwendigen Neuanschaffungen spielen auch die Betriebssysteme eine Rolle. Denn es bieten zwar alle Betriebssysteme – ganz gleich ob macOS und iOS und/oder Windows und Android – mittlerweile einen vergleichbaren Funktionsumfang und Sicherheitsoptionen. Sie unterschieden sich aber in einigen Funktionen, in der Art und Weise, wie die Geräte verwaltet und abgesichert werden, sowie im Preis.

So überzeugen Geräte von Apple beispielsweise durch ihre Update-Policy. Denn in regelmäßigen, meist kurzen Abständen werden neue Features entwickelt und verteilt, durch die etwaige Sicherheitslücken frühzeitig geschlossen und neue Verwaltungs- und Nutzungsmöglichkeiten geschaffen werden. Bei Android-Geräten unterliegen Betriebssystem-Updates hingegen häufig noch individuellen Richtlinien der jeweiligen Gerätehersteller und werden oftmals mit Verzögerung verteilt. Google bietet aber mit der Auszeichnung „Android Enterprise Recommended" ein Gütesiegel an, das Geräte kennzeichnet, die sich besonders für den Unternehmenseinsatz eignen. Das Siegel wird nur dann vergeben, wenn die Geräte – neben anderen notwendigen Voraussetzungen – innerhalb von 90 Tagen System-Updates erhalten. Aufgrund des geschlossenen Ökosystems von Apple ist es zudem deutlich einfacher, eigene Apps für Apple-Hardware zu programmieren, da dies nur für eine begrenzte Anzahl von Modellen geschehen muss. Bei Android-Handys und -Tablets ist dieser Aufwand durch die Vielfalt der Geräte wesentlich höher. Deutlich niedriger hingegen ist meist der Preis der Android- und Windows-Geräte und gerade mit Windows-Geräten sind viele Nutzer auch deutlich vertrauter.

In der Praxis sieht es häufig so aus, dass sowohl iOS- und macOS- als auch Android- und Windows-Geräte zum Einsatz kommen. Die Verwaltung der Geräte wird dadurch zwar komplexer, ist aber dank moderner Technologien gut handhabbar.

## 6 Zentrale Geräteverwaltung

Ganz gleich für welches Nutzungskonzept, welche Betriebssysteme und Gerätetypen sich ein Unternehmen entscheidet – es ist wichtig, anschließend eine Lösung auszuwählen und zu implementieren, mit der die Geräte, Anwendungen und Daten zuverlässig verwaltet und abgesichert werden können. Hierfür eignet sich zum Beispiel der Einsatz eines Unified Endpoint Management-Systems (UEM). Eine solche zentrale Verwaltungssoftware ist unabdingbar, um bei überschaubarem Aufwand für die IT-Abteilung für Sicherheit und Produktivität sorgen zu können.

UEM-Systeme ermöglichen es, Unternehmensdaten und Apps sowie den Zugriff darauf zu verwalten und sensible Daten bei Bedarf vom Gerät zu löschen. Kommt es zu einer Cyberattacke oder zum Verlust des Geräts, können alle wichtigen Daten von der IT sofort remote gelöscht werden. Und auch Updates können zentral verteilt werden. So wird gewährleistet, dass eventuelle Sicherheitslücken zeitnah geschlossen werden. Ein weiterer Sicherheitsfaktor: Mithilfe eines UEM-Systems kann ein eigener App-Store bereitgestellt werden, in dem sich ausschließlich vom Unternehmen freigegebene Apps befinden. So können sichere Apps zur Verfügung gestellt werden, die beispielsweise zum Öffnen wichtiger Dokumente verwendet werden sollen.

## Sicherer Datenverkehr

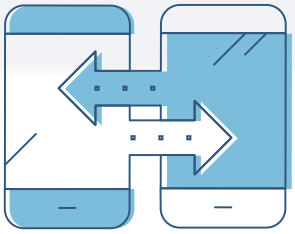
In nächsten Schritt stellt sich die Frage, wie die Geräte im Homeoffice eine sichere Verbindung zu den Anwendungen und Diensten des Unternehmens aufbauen sollen. Als Netzwerk wird vielfach das heimische WLAN genutzt, welches allerdings ein attraktives Einfallstor für Cyberkriminelle darstellt. Die Verbindung zu Unternehmensressourcen sollte daher abgesichert werden – beispielsweise mittels VPN-Client. Solche Lösungen verschlüsseln den Datenverkehr zwischen dem mobilen Endgerät und den IT-Systemen des Unternehmens in Echtzeit und gewährleisten so eine erhöhte Sicherheit.

In einigen UEM-Systemen ist ein VPN-Modul bereits integriert. Es besteht aber ebenfalls die Möglichkeit, Lösungen von Drittanbietern einzubinden. Dies ist häufig sogar sinnvoll, da sie noch zusätzliche Funktionen anbieten, die das mobile Arbeiten nicht nur sicherer, sondern auch produktiver machen. So können sie beispielsweise für eine Optimierung und Stabilisierung von Verbindungen sowie für eine nutzerfreundliche Authentifizierung am VPN-Client und an Cloud-Diensten sorgen, hilfreiche Erkenntnisse für das sogenannte Experience Monitoring liefern und regeln, wann und in welchen Netzen private Apps genutzt werden dürfen.

## Effiziente Kommunikation

Mitarbeiter sollten in Echtzeit miteinander kommunizieren und Informationen austauschen können. Dies ist besonders dann wichtig, wenn Mitarbeiter sich nicht täglich sehen. Die Bereitstellung einer datenschutzkonformen Kommunikationslösung sollte daher auch zur Standardausstattung im Homeoffice gehören. Nur so können die Distanz und der fehlende physische Kontakt von Mitarbeitern untereinander, aber auch zu Geschäftspartnern ausgeglichen werden.

Besonders gut geeignet sind hierfür Videokonferenzlösungen - für den persönlichen Austausch ebenso wie für Team-Meetings oder sogar größere Veranstaltungen. Sie können den persönlichen Austausch zwar nicht 1:1 ersetzen, schaffen aber deutlich mehr Nähe als eine Kommunikation über E-Mails, Chats oder per Telefon. Wichtiger Erfolgsfaktor ist hierbei allerdings, dass die Konferenzen reibungslos ablaufen. Denn nichts ist störender als eine schlechte Audio- und Videoqualität oder sogar Verbindungsabbrüche. Auch wenn die IT auf Heimnetzwerke keinen Einfluss hat, so kann sie mithilfe von modernen VPN-Lösungen allerdings doch für eine gute Verbindungsstabilität sorgen.

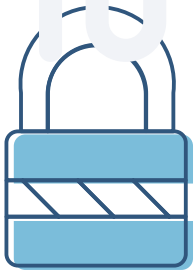


## Zuverlässige Infrastruktur

Interne und externe Systeme sollten hinsichtlich ihrer Erreichbarkeit und Kapazität so aufgestellt sein, dass Anwendungen auch dann reibungslos genutzt werden können, wenn sehr viele oder sogar alle Mitarbeiter aus dem Homeoffice darauf zugreifen. Hierbei ist der Einfluss des Unternehmens je nach Lösung unterschiedlich. So behält die interne IT bei On-Premise-Lösungen, die im Rechenzentrum des Unternehmens installiert sind, zwar die volle Kontrolle über die Daten und IT-Server, die Skalierbarkeit der Lösungen ist hierbei aber häufig begrenzt. Cloud-Lösungen sind hingegen sehr gut skalierbar und können Auslastungsspitzen, wie sie während der Corona-Pandemie vorkamen, flexibel auffangen.

Den hohen Anforderungen an den Datenschutz können viele ebenfalls gerecht werden. Geeignete Cloud-Umgebungen sind unter anderem durch eine entsprechende Zertifizierung, beispielsweise durch ein ISO 27001-Zertifikat, zu erkennen.

10



## Sichere Zugriffe

Der Zugriff auf Daten und Anwendungen des Unternehmens sollte umfassend abgesichert werden. In Zeiten von intelligenten Cyberangriffen und vermehrtem mobilen Arbeiten außerhalb des Unternehmensnetzwerk sind hierfür komplexe Ansätze notwendig – wie zum Beispiel der sogenannte Zero Trust-Ansatz. Dieser sieht vor, dass jede Anwendung, jeder Benutzer und jedes Gerät zunächst als potentielle Bedrohung wahrgenommen wird. Selbst dann, wenn die Zugriffsanfrage aus dem internen Netzwerk stammt.

Anfragen sollen demnach anhand verschiedener Faktoren geprüft werden und auf dieser Basis soll ein entsprechendes Log-In-Verfahren ausgewählt werden. So soll beispielsweise geprüft werden, ob der Zugriff von einem gemanagten Gerät angefordert wird, welches mehr Vertrauen genießt als ein nicht-verwaltetes Gerät. Und auch der Nutzer selbst kann als Kriterium herangezogen werden. Ist er zum Beispiel im Active Directory hinterlegt, wird ihm ein größeres Vertrauen entgegengebracht. Gleiches gilt, wenn der Nutzer auf eine aus dem Firmen-App-Store heruntergeladene App zugreifen möchte, da diese Quelle als sicher gilt. Stammt die App hingegen aus einem öffentlichen App-Store, können zusätzliche Schritte zur Authentifizierung notwendig werden. Ein stärkeres Authentifizierungsverfahren kann beispielsweise die Multi-Faktor-Authentifizierung sein.

Durchsetzen lässt sich dieses Konzept ebenfalls mithilfe eines UEM-Systems. Hier können die beschriebenen Richtlinien definiert und an die Geräte verteilt werden.

11

## Mehr Nutzerfreundlichkeit

Authentifizierungsverfahren wie die Multi-Faktor-Authentifizierung sind für den Nutzer zwar sicher, allerdings häufig zeitaufwändig und im Arbeitsalltag störend. Der Zero Trust-Ansatz kann jedoch nicht nur die Sicherheit erhöhen. Er kann auch für mehr Nutzerfreundlichkeit sorgen. Denn die Richtlinien, die im UEM-System definiert werden, können auch regeln, in welchen Situationen ein Zugriff sogar ganz ohne Passwort gewährt wird. Dies kann beispielsweise dann der Fall sein, wenn ein bekannter Nutzer mit einem verwalteten Gerät, welches über ein entsprechendes Zertifikat verfügt, auf eine App aus dem Unternehmens-App-Store zugreifen möchte. So lässt sich sowohl die benötigte Datensicherheit als auch eine hohe Nutzerfreundlichkeit erreichen. Beides ist beim mobilen Arbeiten enorm wichtig.

12

## Sensibilisierung der Mitarbeiter

Wenn alle Rahmenbedingungen geschaffen sind, sollten im nächsten Schritt die Mitarbeiter „abgeholt“ werden. Denn ein weiterer wichtiger Baustein für eine erfolgreiche Homeoffice-Strategie ist die Aufklärung und Sensibilisierung der Mitarbeiter hinsichtlich des effektiven und sicheren Umgangs mit mobilen Endgeräten. Unternehmen sollten Nutzer daher darin schulen, zu Hause mit Bedacht zu agieren und Angriffe außerhalb des Unternehmensnetzwerkes zu erkennen. Es empfiehlt sich, verbindliche Richtlinien und Tipps für den Umgang mit mobilen Endgeräten im Homeoffice aufzustellen. Diese sollten beispielsweise auf folgende Fragen Antworten geben: Wie kann ich auf Unternehmensressourcen zugreifen? Was darf auf den Geräten gespeichert werden? Welche Apps dürfen heruntergeladen werden? Welche Netzwerkverbindungen sind außerhalb des Firmengeländes zu nutzen? Dieses Regelwerk wird gerade Homeoffice-Neulingen den Einstieg erleichtern.

# Beratung und Support rund um Homeoffice und Remote Work

Wir stehen Ihnen mit unserer Expertise und verschiedenen technologischen Lösungen zur Seite und begleiten Sie dabei, ein Homeoffice-Modell in Ihrem Unternehmen einzuführen oder dieses weiterzuentwickeln und stehen Ihnen während jeder Projektphase zur Seite.


+ 49 221 474 550
+ 1 310 980 2781

sales@ebf.com

www.ebf.com


**Jetzt kontaktieren**
ebf.com/kontakt

## Über EBF

**Ihr Advisor für den Digital Workplace und Enterprise Mobility**

*EBF ist Spezialist für den Arbeitsplatz der Zukunft. Gemeinsam mit unseren Kunden und Partnern erarbeiten wir Lösungen für komplexe Enterprise Mobility-Herausforderungen und erstellen individuelle Konzepte für den digitalen Arbeitsplatz.*
*Unsere Produkte, Services und Lösungen machen digitales, mobiles und flexibles Arbeiten möglich und erhöhen die Produktivität und Effizienz von Mitarbeitern und Unternehmen – unter Einhaltung höchster Sicherheits- und Datenschutzstandards, bei überschaubarem Aufwand für die IT, mit einem positiven Erlebnis für den Nutzer. So wird der Digital Workplace in Unternehmen Realität.*